# UNITED STATES DISTRICT COURT
# EASTERN DISTRICT OF TEXAS

**Civil Action No. 4:22-cv-00249-ALM**

DIVYA GADASALLI, an individual,

Plaintiff,

v.

JERRY BULASA, an individual;
DONG LIAN, an individual; DANYUN LIN, an individual;
TD BANK, N.A., a national banking association;
ABACUS FEDERAL SAVINGS BANK, a federal savings bank;
BINANCE HOLDINGS, LTD. d/b/a Binance, a foreign company;
POLONIEX, LLC, a Delaware limited liability company; and
POLO DIGITAL ASSETS, LTD., a foreign company,

Defendants.
_____/

## AMENDED COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF

Plaintiff DIVYA GADASALLI, an individual (hereafter referred to as "Plaintiff"), by and through undersigned counsel, hereby sues Defendants JERRY BULASA, an individual; DONG LIAN, an individual; DANYUN LIN, an individual; TD BANK, N.A., a national banking association; ABACUS FEDERAL SAVINGS BANK, a federal savings bank; BINANCE HOLDINGS, LTD. d/b/a Binance, a foreign company; POLONIEX, LLC, a Delaware limited liability company; and POLO DIGITAL ASSETS, LTD., a foreign company; for damages and equitable relief. As grounds therefor, Plaintiff alleges the following:

## PRELIMINARY STATEMENT

1. This action arises from a highly-sophisticated and fraudulent paramour scheme -- a "sha zhu pan" or "pig butchering" scam -- that sought to, and ultimately did, steal from Plaintiff a sum greater than Eight Million Dollars ($8,000,000.00).

2. "Sha zhu pan" is a Chinese phrase that is translated to English as "pig butchering" to describe the process in which the offender builds a relationship with the victim over months -- frequently romantic, in which the offender showers the victim with messages of love and affection to emotionally "fatten them up" -- similar to fattening a pig, before enticing the victim to invest in a fake company and, metaphorically, slaughtering the victim.

3. Plaintiff was victimized by such a scam.

4. After meeting online on popular dating service Tinder and communicating frequently via the multi-platform messaging app WhatsApp, Plaintiff and JERRY BULASA ("Defendant BULASA") sparked and built what appeared to Plaintiff to be a deeply-held affection for, and interest in, one another.

5. As their relationship progressed and Plaintiff's trust in Defendant BULASA grew deeper Defendant BULASA -- with false promises of romance and of financial prosperity through cryptocurrency investments -- induced from Plaintiff monetary transfers with financially devastating results.

6. In all, Defendant BULASA induced from Plaintiff monetary transfers in a total sum that exceeds Eight Million Dollars ($8,000,000.00).

7. To effectuate his scheme, Defendant BULASA enlisted Defendants DONG LIAN and DANYUN LIN to assist in receiving from Plaintiff fraudulently procured wire transfers to bank accounts Defendants LIAN and LIN maintained at TD BANK, N.A. and ABACUS FEDERAL SAVINGS BANK -- wire transfers that were ultimately placed under Defendant BULASA's control.

8. Just a few short months after Plaintiff had transferred her funds and cryptocurrency holdings to Defendant BULASA's control, the $8,000,000.00 in fiat currency and cryptocurrency amassed with those funds were stolen from Plaintiff by Defendant BULASA.

9. As a result of Defendants' negligent and/or fraudulent behavior, Plaintiff has suffered grave economic harm for which she seeks compensatory relief.

## PARTIES, JURISDICTION, AND VENUE

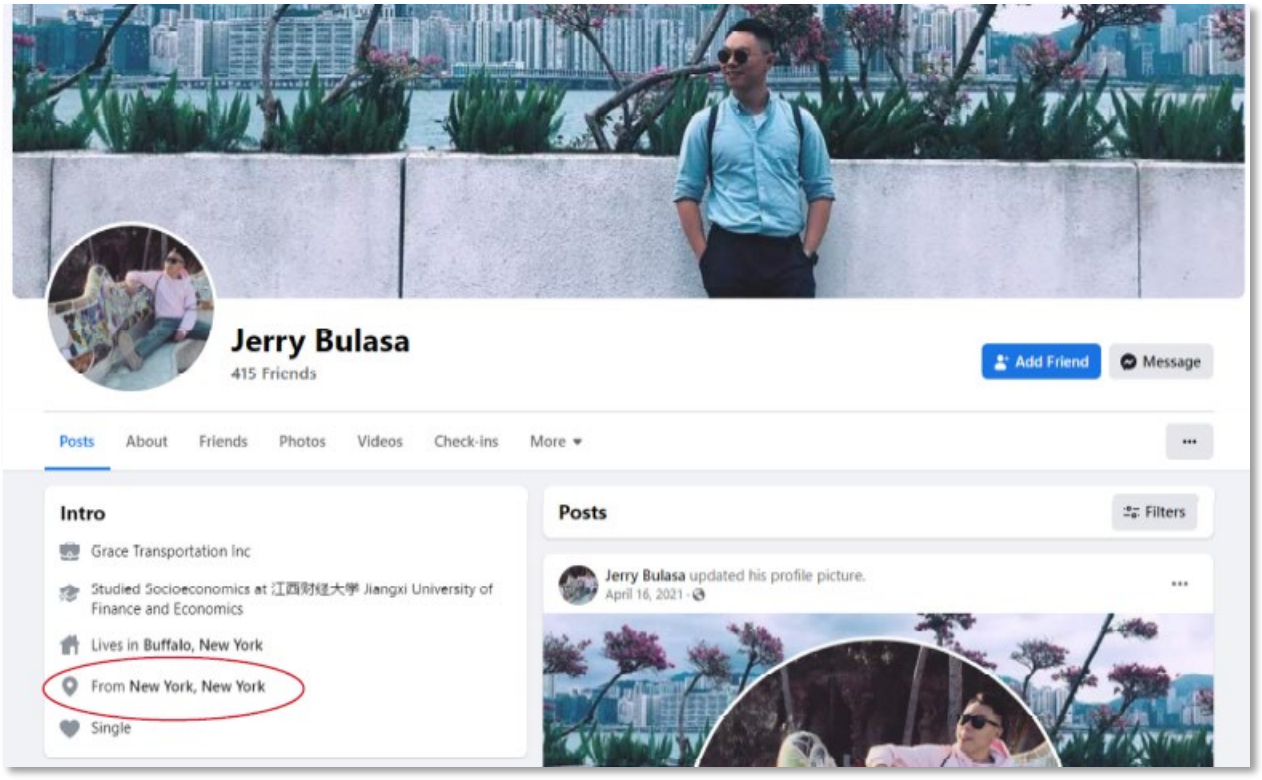
### THE PARTIES

### Plaintiff

10. Plaintiff DIVYA GADASALLI is an individual domiciled in Plano, Texas, is a citizen of the state of Texas, and is *sui juris*.

### Defendants

11. Defendant JERRY BULASA is an individual of Chinese heritage believed to be domiciled in New York, New York, and is *sui juris*. According to his self-published social media profile, Defendant BULASA is from New York, NY.




Although his Facebook profile also indicates that he "*lives in Buffalo, New York*," Defendant BULASA represented to Plaintiff that he actually lives in Brooklyn, New York and works in New York City.



SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

12. Defendant DONG LIAN ("Defendant LIAN") is an individual believed to be domiciled in New York, New York and is *sui juris*.

13. Defendant DANYUN LIN ("Defendant LIN") is an individual believed to be domiciled in New York, New York and is *sui juris*.

14. Upon information and belief, Defendant BULASA, Defendant LIAN, and Defendant LIN might be the same person or, in the alternative, are three individuals who conspired with one another to perpetrate upon Plaintiff the fraud detailed herein.

15. Defendant TD BANK, N.A. ("TD BANK") is a national banking association federally chartered pursuant to the National Bank Act (12 U.S.C. § 38, *et seq.*) and supervised by the federal Office of the Comptroller of the Currency. TD BANK's principal place of business is in Cherry Hill, New Jersey. Furthermore, TD BANK is a subsidiary of THE TORONTO DOMINION BANK and a member of the family of companies collectively known as "TD BANK GROUP."

16. Defendant ABACUS FEDERAL SAVINGS BANK ("ABACUS BANK") is a federal savings bank with its headquarters in New York, New York. According to its website, ABACUS BANK was founded to provide financial services to immigrants and local residents of lower Manhattan. The bank now has six (6) branches covering New York, New Jersey and Pennsylvania. ABACUS BANK provides deposit services, safe deposit boxes and loans for both residential and commercial real estate properties to its communities.

17. Defendant BINANCE HOLDINGS, LTD. d/b/a Binance ("BINANCE") is a foreign company which, upon information and belief, is registered and headquartered with its principal place of business in the Cayman Islands, though it professes to not have a principal executive office.[1]

[1] Paddy Baker, *Binance Doesn't Have a Headquarters Because Bitcoin Doesn't, Says CEO,* COINDESK (May 8, 2020), https://www.coindesk.com/binance-doesnt-have-a-headquarters-because-bitcoin-doesnt-says-ceo.

BINANCE is a digital currency wallet and money transmitter services platform where merchants and consumers exchange digital currencies like bitcoin and Ether.

18. BINANCE refers to itself as an "ecosystem" comprising several interrelated components. The company's Terms of Service define BINANCE as follows:

> **Binance** refers to an ecosystem comprising Binance websites (whose domain names include but are not limited to https://www.binance.com), mobile applications, clients, applets and other applications that are developed to offer Binance Services, and includes independently-operated platforms, websites and clients within the ecosystem (*e.g.*, Binance's Open Platform, Binance Launchpad, Binance Labs, Binance Charity, Binance DEX, Binance X, JEX, Trust Wallet, and fiat gateways).

Among the platforms/websites/fiat gateways within the BINANCE ecosystem is Binance.US, which serves customers in the United States, including in this jurisdiction. Collectively, all of these components of the "ecosystem" constitute BINANCE.

19. Additionally, numerous public reports have identified BINANCE as perhaps the largest vehicle in the world through which stolen cryptocurrency assets are laundered by U.S. residents, *to wit*:

> Binance Holdings Ltd. is under investigation by the [United States] Justice Department and Internal Revenue Service, ensnaring the world's biggest cryptocurrency exchange in U.S. efforts to root out illicit activity that's thrived in the red-hot but mostly unregulated market.
>
> * * *
>
> The firm, like the industry it operates in, has succeeded largely outside the scope of government oversight. Binance is incorporated in the Cayman Islands and has an office in Singapore but says it lacks a single corporate headquarters. Chainalysis Inc., a blockchain forensics firm whose clients include U.S. federal agencies, concluded last year that among transactions that it examined, more funds tied to criminal activity flowed through Binance than any other crypto exchange..

20. Furthermore, BINANCE publicly announced in January 2022 that it was teaming up with the National Cyber-Forensics and Training Alliance (NCFTA) -- an American non-profit entity with offices in spanning across the United States -- to "fight against cybercrime, ransomware, and

terrorism financing."[2] According to Tigran Gambaryan, Vice President of Global Intelligence and Investigations at BINANCE:

> Joining the NCFTA is an important step in our joint fight against cybercrime, securing the cryptocurrency ecosystem for the entire community. Binance aims to be the leading contributor in the fight against cybercrime, ransomware, and terrorism financing. We will continue our fight against cybercrime and increase our level of cooperation and transparency through our partnership with the NCFTA.[3]

The press release related to this announcement even states: "To date, Binance has cooperated with hundreds of criminal investigations, which have led to high-profile arrests, including a cybercriminal group laundering $500M in ransomware proceeds."[4] "Cooperation" only takes place voluntarily, which BINANCE clearly has done in "hundreds of criminal investigations" and through its "partnership" with the American-based NCFTA and its activities throughout the United States, including -- upon information and belief -- within this jurisdiction

21. At all times material hereto, Defendant BULASA has maintained -- and continues to maintain as of the date of this filing -- an account at BINANCE in which Defendant BULASA holds the cryptocurrency stolen from Plaintiff.

22. Defendant POLONIEX, LLC is a Delaware limited liability company with its principal place of business in Boston, Massachusetts. POLONIEX is a wholly-owned subsidiary of Pluto Holdings, Inc. ("Pluto"), a Delaware corporation, which is a wholly-owned subsidiary of Circle Internet Financial Limited ("Circle"), an Irish private company.

---

[2] "NCFTA onboards crypto exchange Binance to fight against cybercrime," *CoinTelegraph*, Jan. 18, 2022, https://cointelegraph.com/news/ncfta-onboards-crypto-exchange-binance-to-fight-against-cybercrime

[3] "Binance Becomes the Blockchain and Cryptocurrency Industry's First to Join the National Cyber-Forensics and Training Alliance (NCFTA)", *PR Newswire*, January 18, 2022, https://www.prnewswire.com/news-releases/binance-becomes-the-blockchain-and-cryptocurrency-industrys-first-to-join-the--national-cyber-forensics-and-training-alliance-ncfta-301462332.html.

[4] *Id.*



**SILVER MILLER**
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

23. Defendant POLO DIGITAL ASSETS, LTD. ("PDAL") is a foreign corporation incorporated under the laws of the Republic of Seychelles.

24. Upon information and belief, POLONIEX, LLC sold its digital asset trading platform to PDAL in November 2019. Notwithstanding the aforementioned sale, POLONIEX, LLC and PDAL are believed to continue to jointly market themselves under the unifying brand "POLONIEX"; and they shall be jointly referred to herein as POLONIEX.

**Other Liable Persons/Entities**

25. In addition to Defendants, there are likely other parties who may be liable to Plaintiff, but about whom Plaintiff currently lacks specific facts to permit her to name these persons or entities as party defendants. By not naming such persons or entities at this time, Plaintiff is not waiving her right to amend this pleading to add such parties, should the facts warrant adding such parties.

**JURISDICTION AND VENUE**

26. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332 because the amount in controversy exceeds Seventy-Five Thousand Dollars ($75,000.00), exclusive of interest, costs and attorneys' fees, and is an action between citizens of different states.

27. This Court has personal jurisdiction over Defendants because they: (a) operate, conduct, engage in and/or do business within this jurisdiction; (b) committed a tort in this jurisdiction; and/or (c) reside in this jurisdiction.

**Specific Jurisdiction**

28. This suit arises out of or relates to Defendants' contacts with this forum.

29. Plaintiff is a resident of Texas, and she suffered harm in part because: (a) Defendant BULASA, Defendant LIAN, and Defendant LIN were together operating a financial scam that ensnared Plaintiff and stole from her several million dollars in fiat currency and cryptocurrency, and (b) BINANCE and POLONIEX's unreasonably lax Anti-Money Laundering ("AML") and "Know

Your Customer" ("KYC") procedures encouraged hackers by providing them a marketplace where they could easily launder stolen digital assets.

30. Plaintiff's claims also involve harm suffered in Texas, as her cryptocurrency assets were stolen and laundered through computer servers in Texas.

31. Plaintiff's claims also arise out of or relate to forum-related activities. For example, Plaintiff's fraudulent inducement and conversion claims arise out of or relate to Defendant BULASA stealing, and BINANCE and POLONIEX taking possession of, Plaintiff's stolen cryptocurrency when it was transferred from Plaintiff's possession in Texas to the BINANCE and POLONIEX exchanges.

32. Exercising jurisdiction over Defendants in this forum is reasonable and comports with fair play and substantial justice.

**General Jurisdiction over Binance**

33. This Court may assert general jurisdiction over a corporation if the corporation is incorporated in Texas, if the corporation has its principal place of business in Texas, or if the corporation's affiliations with Texas are so "continuous and systematic" as to render it essentially at home here.

34. As noted above, BINANCE voluntarily works with American law enforcement agencies to "fight against cybercrime, ransomware, and terrorism financing." Upon information and belief, those law enforcement agencies include some in Texas. For example, the Texas State Securities Board (TSSB) is one of the most active and prominent state-based regulatory bodies in the United States that investigates and prosecutes malfeasant actions by cryptocurrency businesses and harm-inducing actors. In one such prosecution, the TSSB issued a March 2021 "Cease and Desist Order" to prevent a Binance impersonator from operating in Texas under the business names "Binance Assets" and "BinanceAssets LTD" -- an Order that, upon information and belief, was issued with

BINANCE's assistance and approval and which BINANCE's Chief Executive Officer (Changpeng "CZ" Zhao) publicly praised on Twitter on the company's behalf:


35. Moreover, BINANCE uses various third-party companies, including companies located within this judicial district, to enable what BINANCE calls its "ecosystem" to function.

36. BINANCE makes clear in the "Binance Terms of Use" that its users must agree to that it considers its fiat gateways, including Binance.US, to be part of the "ecosystem" that defines "Binance." After expressly defining "Binance" to include "fiat gateways" the Terms of Use also explain that the fiat gateways are part of the services BINANCE provides:

> **Binance Services** refer to various services provided to you by Binance that are based on Internet and/or blockchain technologies and offered via Binance websites, mobile applications, clients and other forms (including new ones enabled by future technological development). Binance Services include but are not limited to such Binance ecosystem components as Digital Asset Trading Platforms, the financing sector, Binance Labs, Binance Academy, Binance Charity, Binance Info, Binance Launchpad, Binance Research, Binance Chain, Binance X, Binance Fiat Gateway, existing services offered by Trust Wallet and novel services to be provided by Binance.

In short, BINANCE's Terms of Use inform consumers that a "Binance Fiat Gateway" -- only one of which is San Francisco-based BAM d/b/a Binance.US -- is a service provided by BINANCE.

37. In February 2022, BINANCE bought a $200 million ownership interest in *Forbes*, which extended BINANCE's influence and its financial interests across the entire United States.

38. The following month (March 2022), BINANCE publicly touted that it was the official cryptocurrency exchange partner for the 64th Annual GRAMMY Awards.

39. BINANCE even served as the sponsor of the April 2022 White House Correspondents' Dinner "Evening of Magical Realism."

40. The footprint of BINANCE's ecosystem is undeniably imprinted across the United States.

41. Furthermore, in February 2022, BINANCE launched several celebrity-fueled advertisements during the Super Bowl to solicit accountholders in the United States, including in this jurisdiction.

42. According to a BINANCE press release:

> The global campaign – featuring global superstar and entrepreneur J Balvin, all-star basketball forward Jimmy Butler and mixed martial arts fighter Valentina Shevchenko – focuses on encouraging consumers to do the research and learn crypto themselves, so they can be empowered and accountable for their own financial freedom and success.
>
> On February 13, the day of the Big Game, for every commercial aired during the game with a celebrity "talking crypto", viewers are encouraged to sound Binance's #CryptoCelebAlert at CryptoCelebAlert.com to claim one of 2,222 POAP NFTs featuring Jimmy Butler. More importantly, they can access an easy-to-read crypto primer to better understand the basics of crypto.[5]

43. Jimmy Butler, one of the featured celebrities promoting BINANCE, was born and raised in Houston, TX and played part of his collegiate basketball career in Texas. He now has over 6,500,000 followers on Instagram, more than 2,500,000 followers on Facebook, and more than 800,000 followers on Twitter.

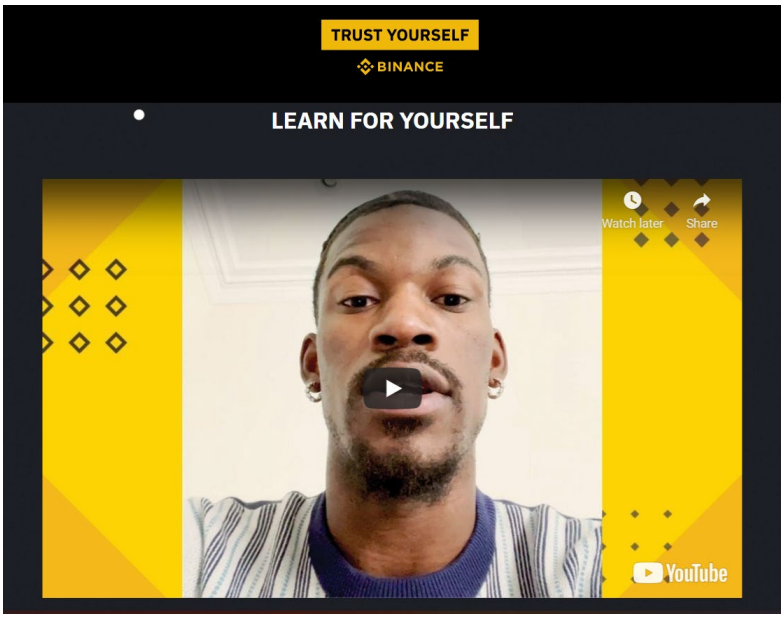
---

[5] https://www.binance.com/en/blog/community/binance-unites-j-balvin-jimmy-butler-and-valentina-shevchenko-to-take-on-big-game-crypto-ads-invites-fans-to-sound-the-cryptocelebalert-and-trust-themselves-to-learn-crypto-421499824684903392.



**SILVER MILLER**
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

44. As Mr. Butler himself espouses in the advertising video on CryptoCelebAlert.com: "*BINANCE and I, we're here to tell you: Trust yourself, and do your own research.*"




Mr. Butler -- a basketball celebrity with a legion of fans across Texas and elsewhere -- is clearly promoting BINANCE's business interests in this jurisdiction to his many followers.

45. Technology has opened up new avenues for solicitation. A new means of solicitation, though, is not any less of a solicitation.

46. In addition, many other cryptocurrency owners in the United States use BINANCE's services -- even where those services are not permitted by law and where BINANCE publicly claims it does not provide its services.

47. As reported by *Forbes* on October 29, 2020[6], an internal document leaked to *Forbes* revealed an extensive strategy by BINANCE to achieve its goals of "U.S. enforcement mitigation," to "insulate Binance from U.S. enforcement." Among the strategies revealed in the leaked document

[6] https://www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked-tai-chi-document-reveals-binances-elaborate-scheme-to-evade-bitcoin-regulators/?sh=6056ed842a92.



SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

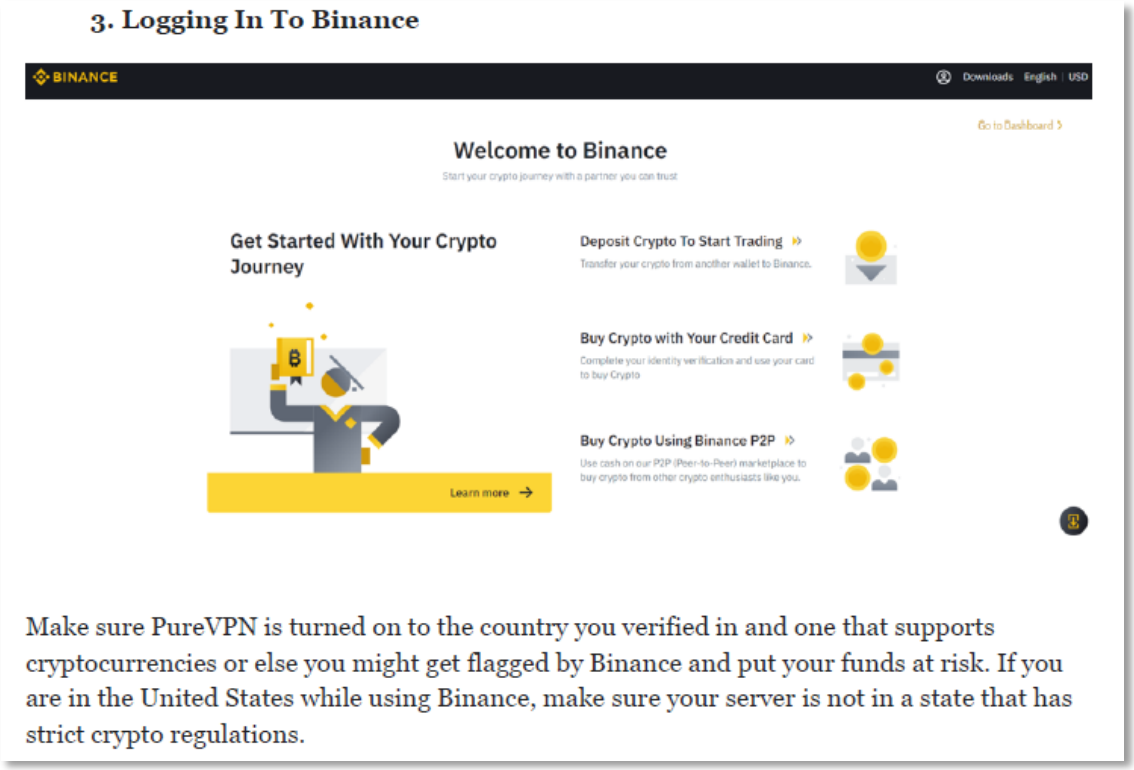
was maintaining that BINANCE has no office, and the strategic use of Virtual Private Networks ("VPNs") to obscure traders' locations as a way to evade regulatory scrutiny.

48. While BINANCE publicly claims it does not permit United States-based customers to use its services -- something it purports to monitor by tracking the geo-location of the IP Address used by the customer to login to BINANCE -- that supposed barrier is easily overcome through methods of which BINANCE is well-aware and which BINANCE tacitly permits.

49. To evade geo-location tracking monitors, a customer need only use a VPN that spoofs the user's actual location. Instead of marking his/her IP Address with a location in the United States, the BINANCE user employs a VPN so that BINANCE's records will reflect that the user is logging in from a non-U.S. territory that is supported by BINANCE.

50. One such VPN is PureVPN, which describes the simple process thusly:


51. As PureVPN explains, as long as the location the user choose through his/her VPN is a non-U.S. country supported by BINANCE, the user's log-in to BINANCE will proceed unfettered:




52. BINANCE is readily aware that U.S.-based users -- including those based within this jurisdiction -- utilize VPN services to access BINANCE; and BINANCE does not prevent such use.

53. In fact, as referenced in the *Forbes* October 2020 article, the leaked BINANCE internal document explicitly calls for the "strategic" use of VPNs that obscure traders' locations as a way to evade regulatory scrutiny by U.S. governmental regulators. In addition to a guide to using VPNs on BINANCE's website, CZ has in multiple instances advocated for VPN use as a way to obscure a BINANCE user's location. In a June 2, 2019 tweet, he wrote that "VPNs [are] a necessity, not optional."

54. To the extent BINANCE claims it has no or few users in this jurisdiction, that claim is belied by the number of BINANCE accountholders in this jurisdiction who take simple steps (well known to BINANCE) to evade BINANCE's lax barriers to entry.

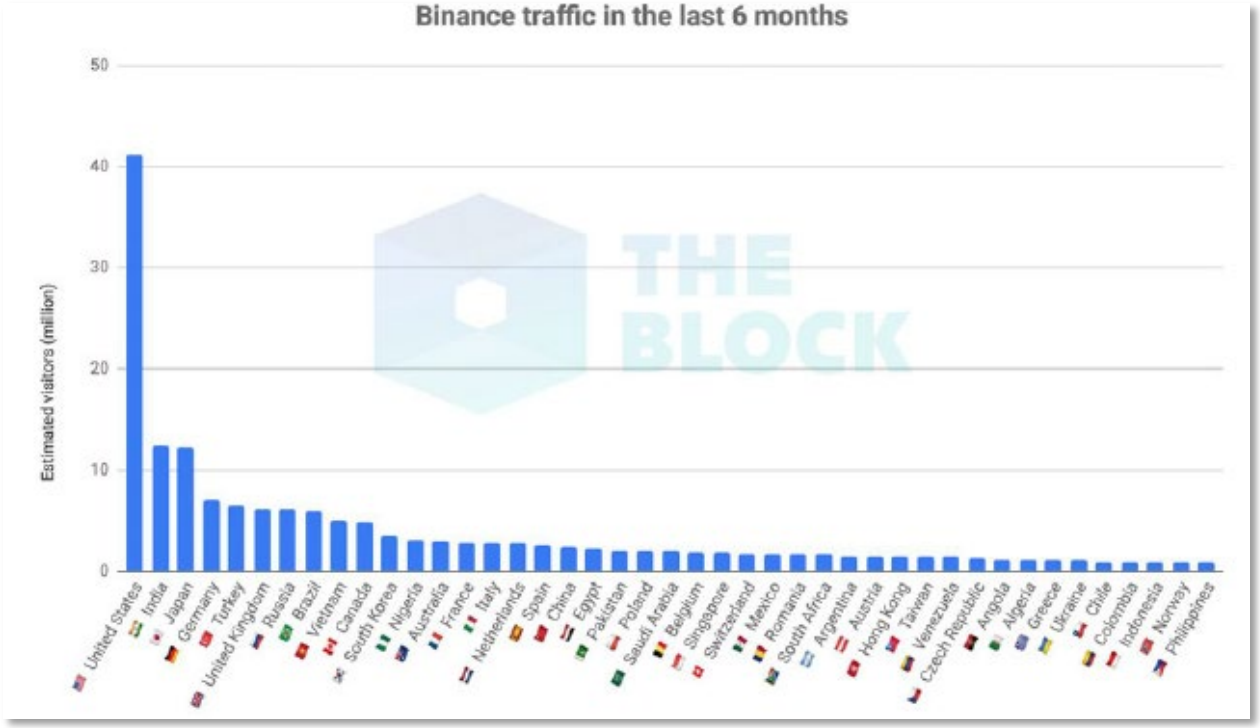
55. A July 2021 report by Inca Digital (a data firm whose technology is used by the U.S. Commodity Future Trading Commission for investigations and market surveillance) highlighted this

fact by noting that hundreds of Americans use VPNs to trade cryptocurrency on BINANCE in a manner that is "an open secret in the industry."

56. Upon information and belief, even document production from BINANCE would not definitively demonstrate that U.S.-based users do not use VPNs to access BINANCE's platforms, as it is not believed that BINANCE tracks such things; and IP Address records for BINANCE users are often tainted with spoofed IP Addresses through this simple method of entry.

57. By early 2018, BINANCE had become the world's biggest cryptocurrency exchange. It had more than 5,000,000 users in January 2018, 10,000,000 users by July 2018, and 15,000,000 users by the end of 2019. In June 2018, *Forbes* reported that 38% of BINANCE's traffic came from customers in the United States -- more than from any other nation.

58. BINANCE's growth continued in 2019. A June 2019 article published by *The Block*, which researches and analyzes digital assets, included the following chart reflecting Binance.com's website traffic for the preceding six months.






SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

59. Likewise, according to data compiled by SimilarWeb, a company that tracks website traffic to millions of websites, the United States was second only to Russia in December 2020 in website traffic to the Binance.com website.

60. Because of its large U.S. customer base, BINANCE was concerned about its global operations having to strictly comply with U.S. AML requirements. Unwilling to subject BINANCE's entire operation to regulatory scrutiny by U.S. governmental agencies -- yet unwilling to give up its lucrative U.S. customer base -- BINANCE devised a plan to create a U.S. "on ramp" to BINANCE's cryptocurrency exchange that would enable U.S. users to convert fiat (*e.g.*, U.S. Dollars) to cryptocurrency and subject only the "on ramp" entity to U.S. AML requirements.

61. BINANCE's plan was to have a U.S. business that would serve as a U.S. "on ramp" to BINANCE's exchange and would expose that U.S. company, rather than BINANCE, to U.S. regulations. Rather than select an existing U.S. company to partner with, BINANCE decided to create one instead. As a result, BINANCE, or those acting upon the instructions of BINANCE or its owner (Changpeng Zhao) created BAM Trading Services Inc. d/b/a Binance.US. Binance.US was specifically formed to enable BINANCE to retain its U.S. user base while simultaneously trying to minimize the risk of exposing BINANCE to regulation by U.S. authorities.

62. Although Binance.US is but one entity in the BINANCE ecosystem, the relationship between the two essentially makes BINANCE at home in the United States, including in this jurisdiction.

63. BAM Trading Services Inc. was incorporated in the State of Delaware in early 2019, and its headquarters are located in San Francisco, California. BAM does business throughout the United States as "Binance.US." Binance.US has not revealed who owns it, why it was created, or how it was capitalized at startup. This information is unavailable to Plaintiff.

64. Upon information and belief, CZ is the principal owner of BINANCE and the principal, if not sole, owner of Binance.US.

65. Although Binance.US is a separately incorporated entity, BINANCE and Binance.US are intertwined to such a degree that Binance.US is an alter ego of BINANCE. This is evidenced by, among other things, the following:

(a) BINANCE has access to Binance.US's books and records, including Binance.US's most sensitive and confidential business information;

(b) BINANCE has the ability to control, and does in fact control, all corporate decision making at Binance.US;

(c) BINANCE provides the technology for the Binance.US on ramp;

(d) BINANCE provides the security practices and branding for Binance.US;

(e) BINANCE controls Binance.US's ability to meet regulatory standards. BINANCE has publicly reiterated that it is controlling the systems that are essential for its fiat on ramps to meet regulatory standards, explaining in a July 28, 2020 statement on the Binance.com website that "*Binance has implemented sophisticated compliance and monitoring systems for its fiat gateways, which include daily monitoring tools such as on-chain monitoring for cryptocurrency transactions.*" Binance.US is one of BINANCE's fiat on ramps;

(f) Upon information and belief, all or a substantial part of the capital used to establish Binance.US and fund its startup came from, or at the direction of, BINANCE or its principal owner and CEO, Changpeng Zhao;

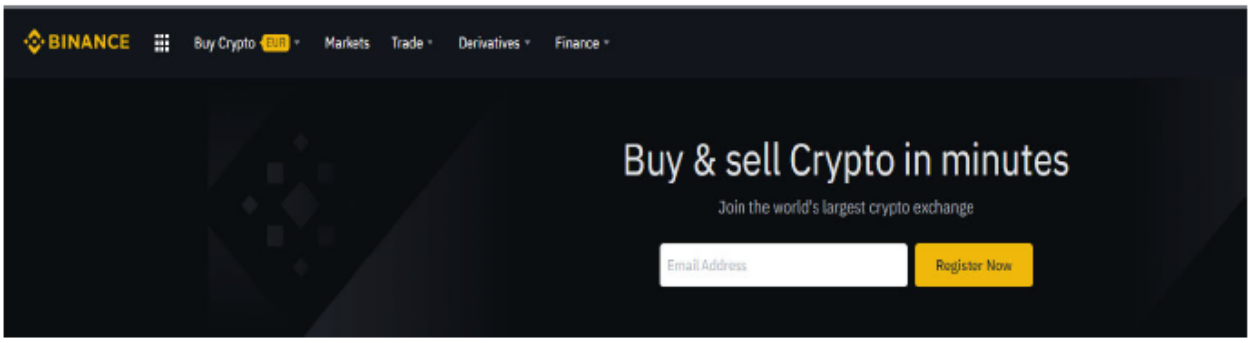
(g) Through its "Terms of Use," captioned "BAM Platform Terms of Use," Binance.US requires its customers who reside in the United States to agree to indemnify and hold harmless entities that include BINANCE and individuals that include BINANCE's owner and CEO;

(h) Upon information and belief, BINANCE has access to Binance.US's user accounts or user information;

(i) Upon information and belief, Binance.US provides BINANCE with information about Binance.US customers; and

(j) BINANCE's Terms of Use inform consumers that a "Binance Fiat Gateway" -- one of which is Binance.US -- is a service provided by BINANCE.

66. The Binance.US website was designed to look like BINANCE's website and to assure users that the two were essentially the same. Here, for example, are historic screenshots of the home page of BINANCE's and Binance.US's websites.





Binance.US's website has even touted that "*Binance.US brings you the trusted technology from the world's leading crypto exchange, Binance.*"

67. Likewise, the colors, fonts, logos, phrasing, images, and position of items on BINANCE's and Binance.US's Facebook pages have been designed to ensure customers believe BINANCE and Binance.US are a coordinated entity.



SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com


68. Treating BINANCE's and Binance.US's identities as entirely separate and divided from one another would result in fraud or injustice.

69. BINANCE used Binance.US as a decoy to feign compliance with U.S. regulations and distract regulators from U.S. trades on BINANCE's platform.

70. As a result of the foregoing, BINANCE controls Binance.US. BINANCE dictates every facet of Binance.US's business, from broad policy decisions to routine matters of day-to-day operation. Binance.US is a mere shell or conduit for the affairs of BINANCE.

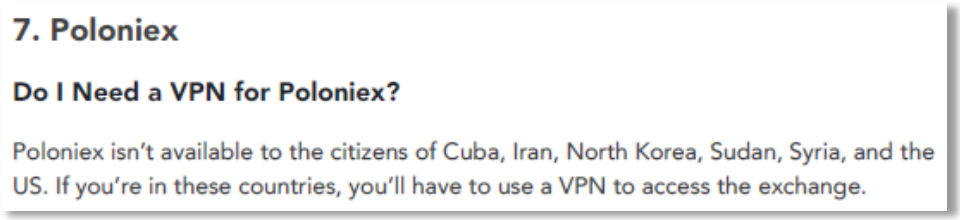
71. Binance.US and BINANCE are alter egos. Thus, Binance.US's contacts with this jurisdiction should be imputed to BINANCE; and jurisdiction over BINANCE in this court would be proper.

**General Jurisdiction over Poloniex**

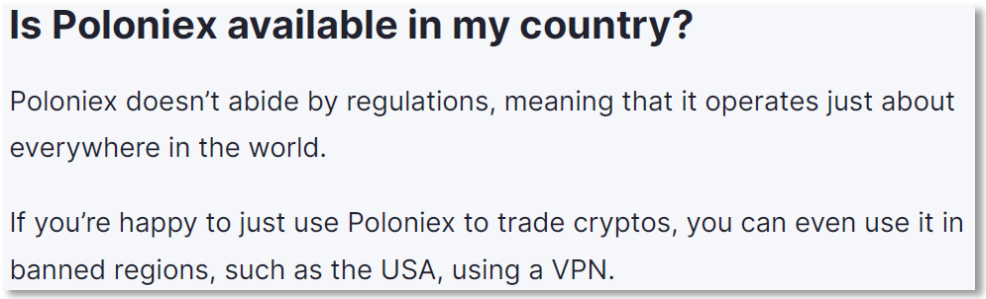
72. POLONIEX is registered with the Financial Crimes Enforcement Network ("FinCEN") as a Money Services Business ("MSB"), registration number 31000091844018. POLONIEX, LLC's parent company Circle Internet Financial, Inc. is also registered with FinCEN as an MSB, registration number 31000110033860.

73. Much like BINANCE has many users in the United States despite public assertions that its services are not available to U.S.-based users, POLONIEX has many cryptocurrency accountholders in the United States who use POLONIEX's services -- even where those services are not permitted by law and where POLONIEX publicly claims it does not provide its services.

74. According to readily-available VPN services, using POLONIEX in the United States is easily accomplished despite POLONIEX's public pronouncements to the contrary:




75. As one site explains:




76. Just as with BINANCE, upon information and belief, even document production from POLONIEX would not definitively demonstrate that U.S.-based users do not use VPNs to access POLONIEX's platforms, as it is not believed that POLONIEX tracks such things; and IP

Address records for POLONIEX users are often tainted with spoofed IP Addresses through this simple method of entry.

77. In light of the foregoing, it is believed that POLONIEX has continuous and systematic connections to the United States, including this forum.

78. Venue of this action is proper in this Court pursuant to 28 U.S.C. § 1391 because the causes of action accrued in this jurisdiction.

## GENERAL FACTUAL ALLEGATIONS

79. In or about May 2021, Plaintiff -- on popular online dating service Tinder -- met a man who claimed his name was JERRY BULASA.

80. Defendant BULASA represented to Plaintiff that he lives and works in New York City, NY, where he assists in running his father's business and takes care of his father, who was purportedly in poor health.

81. Plaintiff and Defendant BULASA quickly developed what appeared to be a mutual personal interest in one another, and they began communicating frequently via the multi-platform messaging app WhatsApp.

82. Their communications also delved into discussions of cryptocurrency investing, with Defendant BULASA soliciting Plaintiff to entrust with him some of her funds so he could help her grow those investments into greater wealth.

83. Defendant BULASA portrayed himself to Plaintiff to be a very successful and savvy cryptocurrency investor; and the investment instructions he induced her to follow were specific down to the hour and minute at which she should place her funds with him, as those times would purportedly provide Plaintiff the best investment outcome.



SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

84. Relying upon the representations of security and profitability Defendant BULASA made to her, Plaintiff used some family funds to invest in cryptocurrency at Defendant BULASA's instruction.

85. Plaintiff, based on Defendant BULASA's representations and advice, wired Three Hundred Ninety-Six Dollars ($396,000.00) to bank accounts at TD BANK and ABACUS BANK purportedly maintained or controlled by Defendants DONG LIAN and DANYUN LIN -- who Defendant BULASA told Plaintiff were investors with whom he worked who already held cryptocurrency in accounts Defendant BULASA oversaw, thusly:

| DATE OF WIRE TRANSFER | BANK | BANK ACCOUNT TO WHICH FUNDS WERE WIRED | NAMED ACCOUNT HOLDER | AMOUNT TRANSFERRED |
|---|---|---|---|---|
| May 13, 2021 | TD BANK | ***8000 | Dong Lian | $10,000.00 |
| May 17, 2021 | ABACUS | ***0334 | Dong Lian | $86,000.00 |
| May 26, 2021 | ABACUS | ***0334 | Dong Lian | $100,000.00 |
| June 2, 2021 | TD BANK | ***2161 | Danyun Lin | $200,000.00 |
| | | | TOTAL | $396,000.00 |

86. Upon information and belief, Defendant BULASA, Defendant LIAN, and Defendant LIN might be the same person or, in the alternative, three individuals who conspired with one another to perpetrate the fraud upon Plaintiff detailed herein.

87. In return for the funds wired to them, Defendant LIAN and Defendant LIN transferred to Plaintiff cryptocurrency, which she then forwarded to a cryptocurrency account controlled by Defendant BULASA so he could invest it in accordance with his purported cryptocurrency expertise.

88. The investment instructions Defendant BULASA provided Plaintiff appeared to be producing positive results, and the personal relationship between Plaintiff and Defendant BULASA was likewise progressing with positive expressions of mutual affection. Based on the trust and

emotional connection she had placed in Defendant BULASA, Plaintiff continued to follow his investment advice.

89. Under Defendant BULASA's guidance, Plaintiff opened a cryptocurrency account at U.S.-based cryptocurrency exchange Coinbase which she funded with additional family monies that were used to purchase cryptocurrency that was subsequently transferred to cryptocurrency investment firm accounts operated by Defendant BULASA.

90. In addition to the May 2021 and early-June 2021 bank wire transfers to Defendant LIAN and Defendant LIN, Plaintiff funded her Coinbase account with approximately Six Million Dollars ($6,000,000.00); used those funds to purchase Tether[7], and then sent those Tether to an investment account allegedly created for Plaintiff that was overseen by Defendant BULASA.

91. According to Defendant BULASA, the external investment account into which Plaintiff's Tether was being deposited was maintained at cryptocurrency investment firm CoinFund, which he represented to Plaintiff had just been renamed Digital Fund.

92. Upon information and belief, CoinFund is a legitimate cryptocurrency investment firm with offices in New York City, NY and Miami, FL that never changed its name to Digital Fund; and Plaintiff never actually maintained an account at CoinFund.

93. Upon further information and belief, Digital Fund is a fake cryptocurrency exchange that served as an engine of theft for Defendant BULASA -- providing him a mechanism to proffer Plaintiff false account statements and real-time values of cryptocurrency markets on legitimate exchanges that masked the fraudulent scheme Defendant BULASA was perpetrating upon Plaintiff.

[7] Tether (often abbreviated with the symbol "USDT") is a cryptocurrency hosted on the Ethereum and Bitcoin blockchains. It is categorized as a "stablecoin," because it was originally designed so that each coin would always be worth One Dollar ($1.00 USD). Thus, one USDT is worth roughly $1.00; and 6,000,000 USDT are worth roughly $6,000,000.00. Tether has one of the largest market caps, and is one of the most widely-circulated cryptocurrencies, in the world.

94. By December 2021, Plaintiff's Digital Fund account had purportedly grown to a value of approximately Ten Million Dollars ($10,000,000.00); however, Defendant BULASA told Plaintiff she was unable to withdraw any of those funds due to obstacles Digital Fund had purportedly implemented.

95. Defendant BULASA -- who also purported to maintain his own account at Digital Fund -- told Plaintiff he had bundled his and Plaintiff's Digital Fund accounts together; and she was unable to withdraw any funds from her account while there remained an outstanding amount of annual fees on Defendant BULASA's account.

96. In December 2021, Plaintiff transmitted Seven Hundred Thousand Dollars ($700,000.00) to satisfy the supposed annual fee encumbrance on her Digital Fund account and another Seven Hundred Thousand Dollars ($700,000.00) to satisfy the supposed annual fee encumbrance on Defendant BULASA's Digital Fund account.

97. Even after Plaintiff had satisfied those purported Digital Fund requirements, Defendant BULASA told Plaintiff that additional hurdles prevented Plaintiff from accessing her invested funds.

98. After transferring approximately another Five Hundred Thousand Dollars ($500,000.00) to access her funds, Defendant BULASA represented to Plaintiff that even more obstacles remained and that Plaintiff would have to contribute several hundred thousand more dollars to unencumber both his and Plaintiff's cryptocurrency portfolios.

99. Frustrated and unable to see any viable way out of the financial hole into which Defendant BULASA had placed Plaintiff, Plaintiff acquiesced and transferred several hundred thousand more dollars to unencumber and access her cryptocurrency.

100. Having already placed approximately Eight Million Dollars ($8,000,000.00) under Defendant BULASA's control -- and sensing that Defendant BULASA could no longer be trusted --

Plaintiff contacted Defendant BULASA to determine how she could uncouple her assets from his and transfer those assets to an account somewhere under her direct control.

101. In response to Plaintiff's inquiry, Defendant BULASA -- in or about February 2022 -- provided multiple, implausible excuses as to why Plaintiff could not retain control over her own assets.

102. Through blockchain analytics tracing the path of Plaintiff's cryptocurrency assets, it has become apparent that Defendant BULASA has stolen all of Plaintiff's assets; and those assets have been transferred to cryptocurrency accounts under Defendant BULASA's sole control or have been liquidated into fiat currency and dissipated by Defendant BULASA.

103. For example, Plaintiff's stolen assets have been traced to the following cryptocurrency wallet addresses at BINANCE and POLONIEX (among others), which are believed to be owned or controlled by Defendant BULASA or an unknown third-party to whom he has transferred those stolen assets and which have been used to launder the assets stolen from Plaintiff:

| # | EXCHANGE | DESTINATION ADDRESS | ASSET TYPE | ASSETS UNDER CLAIM (average confirmed with five separate tracing methodologies; in cryptocurrency unit) |
|---|---|---|---|---|
| 1 | Binance | 9ea12866d4b69b347ffff084fc4bb3b97cc4d4b4 | USDT | 351,456.322587 |
| 2 | Binance | f52fb20441641e2c446c7db9c2ebee9b80611679 | USDT | 138,928.623847 |
| 3 | Binance | 1838f42bc8e28f0799e21501620e5a93dd32f107 | USDT | 126,574.190249 |
| 4 | Binance | 9c9ba31722261aced59373b53cf567ca96243f57 | USDT | 105,389.848449 |
| 5 | Binance | 2944f6937dcf1ef0b4a005619a35c2e4757bcee0 | USDT | 98,964.245785 |
| 6 | Binance | e42bee8902895f6f228e1b20e40a7d410ff508bf | USDT | 93,679.797809 |
| 7 | Binance | b22270560cdec8cf281ea6f87c14cb24037421be | USDT | 89,273.852767 |
| 8 | Binance | e15ba3e0824f97f4b0f841cf030021097eaf2108 | USDT | 87,098.577482 |
| 9 | Binance | 497025d44131d4a261705368f8c1cf4b6025897a | USDT | 58,462.166853 |
| 10 | Binance | 7f90ef04ba3ed5b1f7908d8e0463a6975227d4f8 | USDT | 18,795.819565 |
| 11 | Binance | 1a2893432d0615a0764a311b5d2a6062dc212c9d | USDT | 18,717.887253 |

| | | | | |
|---|---|---|---|---|
| 12 | Binance | 5e65b32ee4f6a63a0678a43f9439eb421457d950 | USDT | 13,903.728216 |
| 13 | Binance | 70fc0e221578f6d47f958cfa2bff1f9320bc6eec | USDT | 8,402.510102 |
| 14 | Binance | 430ddd14ad41c97dd09d8df94e00f3eb65b7c694 | USDT | 4,877.660928 |
| 15 | Binance | 44a11506b275dc619a1c5a20dc8969ea305c8dd7 | USDT | 4,391.864424 |
| 16 | Binance | 88dfbd93f509d0b3dcbfd86ee9d6d036ca199ea5 | USDT | 4,212.498994 |
| 17 | Binance | 1fe77c00c81e32c50494e2c73a1ce945dd7215a0 | USDT | 3,908.191703 |
| 18 | Binance | 7db77e4c967c95a5a9e2ec57ec21788dab481893 | USDT | 2,281.305709 |
| 19 | Binance | 6d6ab7dbc46ab652eaf4b09827e0de9cc18bc364 | USDT | 1,406.698380 |
| | | | TOTAL | 1,230,725.791102 USDT |

| | | | | |
|---|---|---|---|---|
| 1 | Poloniex | 1ArN6zUiCYuyQVrujb5iMUvBXw7HxzYjPo | BTC | 10.11113414 |
| 2 | Poloniex | 14kahPazCQEyEwKmeR5JG8mZh66W9caQqe | BTC | 7.50000000 |
| 3 | Poloniex | 1LQ9Mrbvdv5QFe5Pdzw7sTxHexkpRoHmMN | BTC | 7.312601758 |
| 4 | Poloniex | 12XwnGBjU6Hp4ecVv61tRDSGdW3SXkt8CP | BTC | 6.920274378 |
| 5 | Poloniex | 1CCNdKHhqtdK4ZauZ7PWgFvDBpZ59MXjP2 | BTC | 6.11926921 |
| 6 | Poloniex | 17Z3S2pfJGQj6QH39j1UPfoGJJ2kqkWSem | BTC | 4.45347371 |
| 7 | Poloniex | 13mLXtUtSkvPqU8qAv81njLSwe4DAnCrPR | BTC | 2.976871542 |
| 8 | Poloniex | 1Ko5ntJvnGhUYfTmseFJxBuereCi6TFTfp | BTC | 0.51755494 |
| | | | TOTAL | 45.91117968 BTC[8] |

104. As of the date of this filing, blockchain analytics have traced Plaintiff's stolen funds to and/or through the following cryptocurrency wallet addresses (among others), which are believed to be owned or controlled by Defendant BULASA or an unknown third-party to whom he has transferred those stolen assets and which are believed to still be holding some of the assets stolen from Plaintiff:

[8] As of the date of this filing, 45.91117968 BTC are valued at approximately $1,354,379.80 USD ($29,500.00 per BTC).

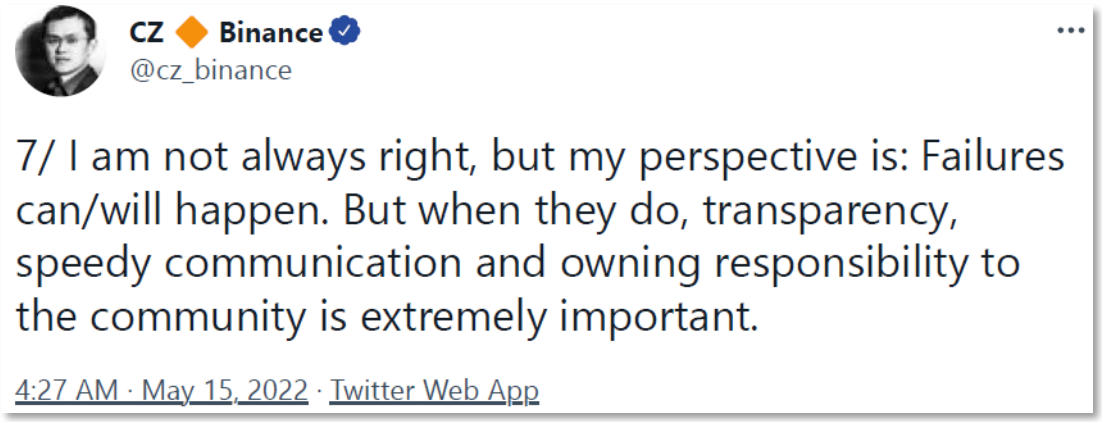


SILVER MILLER
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com

| # | DESTINATION ADDRESS | ASSET TYPE | ASSETS UNDER CLAIM (average confirmed with five separate tracing methodologies; in cryptocurrency unit) |
|---|---|---|---|
| 1 | 365aca59aeb17df6e3a76ec2bdbefe9983f586c5 | USDT | 210,075 |
| 2 | e71010a991fff28c221dfb2aca207c129ff9cf1b | USDT | 86,695.1041952 |
| 3 | 6cca6bde94ad75bfb1e21720677ae9c1f296f607 | USDT | 53,522 |
| 4 | cdce3f15ecb6da711700994fa7c838e45f107f24 | USDT | 49,354.6025112 |
| 5 | f7b7a705d7ac47452eaaff796601271bfc42c43a | USDT | 41,678.0702184 |
| 6 | 3b53e49200546344d7bb31a334e24421a3cb4451 | USDT | 22,359.9849322 |
| 7 | 98022e367dceb0a25317f0e68b949ad3bd7a3571 | USDT | 18,591.4968140 |
| 8 | 2dd59e945a3c036444e37f31d3b2f001d93eefb1 | USDT | 17,020.0423440 |
| 9 | 5fcad1e9ffdc4f207dfe7f0cfdb67d286b0b0162 | USDT | 16,282.1040658 |
| 10 | 7d65a55862aa569f96e31e50c4e6def0b34f05ed | USDT | 7,403.3527816 |
| 11 | 6af4eba5f8b339512960ebef11e02815c42b8c00 | USDT | 5,352.8389960 |
| 12 | 4d27a8e567e4f7b51d1a07ff0cc032d78b0d43d0 | USDT | 3,141.6391760 |
| 13 | 3cb3c884b033fc0dd22c2c8439edd9eeece8818c | USDT | 1,690.8607544 |
| 14 | 12a2dfcac61118e26197ed1a581099faf4dc16e2 | USDT | 655.0425430 |
| 15 | a21675225d76975635cea38b70e874f0a685bf1d | USDT | 414.5838890 |
| 16 | e01d86cf1fa41d6d5d685b3c13555c79fc3aa798 | USDT | 15.9851010 |
| 17 | 5ea54787b09bc81c191a4037f36313d82e407a64 | USDT | 6.3173528 |
| 18 | a2193eb903a185ae3afd05ef461687a221e04adb | USDT | 4.4477338 |
| 19 | 3e362670c657b6e45e792510cd57980466f09194 | USDT | 0.1941922 |
| | | TOTAL | 534,263.6676006 USDT |

105. Defendants BINANCE and POLONIEX were put on notice of the theft and the deposit of Plaintiff's stolen assets into the Destination Addresses listed above. As of the date of this filing, Defendants BINANCE and POLONIEX have not returned to Plaintiff any of those stolen assets and, upon information and belief, have failed to secure those assets from dissipation.

106. BINANCE Chief Executive Officer Changpeng Zhao recently espoused on Twitter his unflinching belief in the importance of "*transparency, speedy communication, and owning responsibility*" when BINANCE does something wrong that harms a member of the cryptocurrency community:




Notwithstanding that public pronouncement, BINANCE has denied Plaintiff everything stated by Mr. Zhao and continues to do so as this litigation progresses and Plaintiff's harm deepens.

107. As a result of the misrepresentations and fraud perpetrated upon her by a would-be paramour and those individuals and entities that fostered his theft and absconding with Plaintiff's assets, Plaintiff has suffered damages, including but not limited to:

(a) Eight Million Dollars ($8,000,000.00) in principal;

(b) Lost profits;

(c) Interest; and

(d) Costs and Expenses.

Plaintiff will be prepared to demonstrate her damages more fully at trial.

108. Plaintiff duly performed all of her duties and obligations, and any conditions precedent to Plaintiff bringing this action have occurred, have been performed, or else have been excused or waived.

109. To enforce her rights, Plaintiff has retained undersigned counsel and is obligated to pay counsel a reasonable fee for its services.

## COUNT I – FRAUDULENT INDUCEMENT
### [AGAINST DEFENDANT BULASA]

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 109 above, and further alleges:

110. Commencing in or about May 2021, Defendant BULASA made multiple representations and statements to Plaintiffs, including but not limited to the following:

(a) Plaintiff would be wise to invest funds in cryptocurrency;

(b) Defendant BULASA was qualified to facilitate Plaintiff's investments in cryptocurrency;

(c) Plaintiff could trust Defendant BULASA to safely manage or oversee the cryptocurrency assets Plaintiff would be purchasing; and

(d) Defendant BULASA was, at all times, acting in Plaintiff's best interest.

111. While making the above-referenced representations to Plaintiff, Defendant BULASA purposely withheld from her the following:

(a) Defendant BULASA was not qualified to facilitate Plaintiff's investments in cryptocurrency;

(b) Defendant BULASA could not be trusted to safely manage or oversee the cryptocurrency assets Plaintiff would be purchasing;

(c) Defendant BULASA would obstruct Plaintiff's efforts to recover her lost assets if anything should go wrong with Plaintiff's investments; and

(d) Defendant BULASA was simply operating an investment scam aimed at stealing Plaintiff's funds.

112. Plaintiff relied on the above-listed material misrepresentations and omissions of material fact in deciding to entrust her funds to Defendant BULASA.

113. Contrary to the representations made to Plaintiff, Defendant BULASA could not be trusted to safely manage or oversee the cryptocurrency assets in which Plaintiff invested.

114. Defendant BULASA intended to induce Plaintiff into sending her funds to Defendant BULASA's control by making these material misrepresentations and omissions, thereby causing Plaintiff to rely upon those statements and omissions of material fact.

115. Plaintiff reasonably and justifiably relied on Defendant BULASA's statements and omissions of material facts.

116. As a direct and proximate result of Plaintiff's reliance on the statements and omissions of material facts made by Defendant BULASA, Plaintiff suffered damage.

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands entry of a judgment against Defendant JERRY BULASA, an individual; for damages, including principal, interest, lost profits, expenses, and any other relief the Court deems proper.

## COUNT II – NEGLIGENT MISREPRESENTATIONS
**[AGAINST DEFENDANT BULASA]**

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1 - 109 above, and further alleges:

117. Commencing in or about May 2021, Defendant BULASA made multiple representations and statements to Plaintiffs, including but not limited to the following:

(a) Plaintiff would be wise to invest funds in cryptocurrency;

(b) Defendant BULASA was qualified to facilitate Plaintiff's investments in cryptocurrency;

(c) Plaintiff could trust Defendant BULASA to safely manage or oversee the cryptocurrency assets Plaintiff would be purchasing; and

(d) Defendant BULASA was, at all times, acting in Plaintiff's best interest.

118. While making the above-referenced representations to Plaintiff, Defendant BULASA purposely withheld from her the following:

(a) Defendant BULASA was not qualified to facilitate Plaintiff's investments in cryptocurrency;

(b) Defendant BULASA could not be trusted to safely manage or oversee the cryptocurrency assets Plaintiff would be purchasing;

(c) Defendant BULASA would obstruct Plaintiff's efforts to recover her lost assets if anything should go wrong with Plaintiff's investments; and

(d) Defendant BULASA was simply operating an investment scam aimed at stealing Plaintiff's funds.

119. Plaintiff relied on the above-listed material misrepresentations and omissions of material fact in deciding to entrust her funds to Defendant BULASA.

120. Contrary to the representations made to Plaintiff, Defendant BULASA could not be trusted to safely manage or oversee the cryptocurrency assets in which Plaintiff invested.

121. Defendant BULASA intended to induce Plaintiff into sending her funds to Defendant BULASA's control by making these material misrepresentations and omissions, thereby causing Plaintiff to rely upon those statements and omissions of material fact.

122. Plaintiff reasonably and justifiably relied on Defendant BULASA's statements and omissions of material facts.

123. As a direct and proximate result of Plaintiff's reliance on the statements and omissions of material facts made by Defendant BULASA, Plaintiff suffered damage.

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands entry of a judgment against Defendant JERRY BULASA, an individual; for damages, including principal, interest, lost profits, expenses, and any other relief the Court deems proper.

## COUNT III – CONVERSION
**[AGAINST DEFENDANT BULASA]**

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-109 above, and further alleges:

124. At all times material hereto, Plaintiff owned and had the right to immediately possess the cryptocurrency assets Defendant BULASA represented to her that he had secured for her in a Digital Funds account -- not just a mere right to payment for the value of those assets -- that was

taken from her and transferred to, *inter alia*, the accounts owned or controlled by Defendant BULASA or an unknown third-party to whom he has transferred those stolen assets.

125. When the stolen cryptocurrency assets were deposited by Defendant BULASA into cryptocurrency wallets he controlled, Defendant BULASA intentionally took possession of and assumed control over Plaintiff's assets.

126. Defendant BULASA has intentionally exercised control, and continues to exercise control, over Plaintiff's cryptocurrency assets in such a way as to exclude Plaintiff from using or possessing those assets.

127. Defendant BULASA knew the property he received was stolen or obtained in a manner constituting theft.

128. As such, Defendant BULASA wrongfully converted Plaintiff's cryptocurrency assets.

129. Defendant BULASA -- through actual fraud, misappropriation, conversion, theft, or other questionable means -- obtained Plaintiff's cryptocurrency, which in equity and good conscience Defendant BULASA should not be permitted to hold.

130. The cryptocurrency assets at issue are specific, identifiable property and can be traced in assets of Defendant BULASA's account(s) at BINANCE, POLONIEX, and elsewhere.

131. As a direct and proximate result of the foregoing, Plaintiff suffered the wrongful conversion of personal property whose value exceeds Seventy-Five Thousand Dollars ($75,000.00).

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands entry of a judgment against Defendant JERRY BULASA, an individual; for damages, including principal, interest, lost profits, expenses, and any other relief the Court deems proper.

## COUNT IV – CIVIL CONSPIRACY
### [AGAINST DEFENDANTS BULASA, LIAN, LIN, BINANCE, AND POLONIEX]

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-109 above, and further alleges:

132. In or around May 2021 and June 2021, Defendant BULASA, Defendant LIAN, and Defendant LIN agreed and combined to engage in a conspiracy in the following manner:

(a) Defendant BULASA falsely induced Plaintiff to deposit with Defendants LIAN and LIN a certain amount of funds for which the three defendants represented they would, in turn, provide Plaintiff with a certain amount of cryptocurrency;

(b) Defendant BULASA instructed Plaintiff to deposit funds into accounts at different banks (TD Bank and Abacus Bank) purportedly under Defendant LIAN's and Defendant LIN's control;

(c) After receiving Plaintiff's wire transfer deposits, Defendant LIAN and Defendant LIN transferred to Defendant BULASA -- not to Plaintiff -- a certain amount of cryptocurrency that Defendant BULASA would purport to safeguard for Plaintiff;

(d) The amount of cryptocurrency transferred by Defendant LIAN and Defendant LIN in return for Plaintiff's deposit was less than the cash equivalent for which Plaintiff had paid; and

(e) After Plaintiff had deposited the funds as instructed, Defendant BULASA would then forever forestall Plaintiff's ability to access that cryptocurrency, which Defendant BULASA actually converted to his own possession.

133. As explained below, Defendants BINANCE and POLONIEX also combined with Defendant BULASA to play vital roles in the conspiracy to steal, launder, and dissipate Plaintiff's cryptocurrency assets.

134. The participants in the conspiracy put their own pecuniary interests ahead of the welfare and economic safety of victim of the conspiracy: Plaintiff.

135. Defendant BULASA, Defendant LIAN, and Defendant LIN agreed to launder the cryptocurrency assets stolen from Plaintiff.

136. Defendant LIAN and Defendant LIN -- acting in concert with Defendant BULASA -- allowed their bank accounts to be used as conduits of fraud and were financially rewarded for their participation in the conspiracy.

137. Moreover, Defendant BULASA, Defendant LIAN, and Defendant LIN -- along with Defendants BINANCE and POLONIEX -- knew that this process of thievery would ultimately place Plaintiff's stolen assets beyond her reach.

138. In the instant matter, Defendants BINANCE and POLONIEX have permitted criminal activity by allowing their custodial vaults and exchanges to serve as shelters for thieves like Defendant BULASA to store purloined assets.

139. In addition, Defendants BINANCE and POLONIEX rendered substantial assistance to Defendant BULASA by ignoring their own internal policies and procedures and by knowingly maintaining inadequate KYC/AML policies which enable skillful cryptocurrency hackers and thieves such as Defendant BULASA to steal cryptocurrency and launder it through the BINANCE ecosystem, as well as at POLONIEX, without providing valid or sufficient personal identification that would enable Plaintiff to retrieve her stolen assets.

140. There is a simple reason why Defendant BULASA laundered the digital loot he stole through Defendants BINANCE and POLONIEX: despite being large cryptocurrency exchanges, Defendants BINANCE and POLONIEX's KYC and AML protocols are lax and do not measure up to industry standards. Defendant BULASA was able to launder the bitcoin stolen from Plaintiff through BINANCE and POLONIEX because BINANCE and POLONIEX failed to implement security measures that were standard throughout the industry.

141. By participating in the conspiracy, Defendants BINANCE and POLONIEX were able to collect significant transaction fees; and, more broadly, BINANCE and POLONIEX were able to further their cultivated image as promoters of anonymous and unregulated financial transactions,

which attracts fraudsters and other transacting parties seeking to evade scrutiny and drives revenue and profits for BINANCE and POLONIEX.

142. Defendants BINANCE and POLONIEX's failure to comply with their obligations concealed Defendant BULASA, Defendant LIAN, and Defendant LIN's fraud, enabled those individual defendants to continue their illegal activity and dissipate the proceeds of the crime, and enabled BINANCE and POLONIEX to continue to earn significant fees from these transactions.

143. Defendants BINANCE and POLONIEX each knew that their KYC and AML policies and procedures -- including any tracing analysis of where funds originated -- were inadequate, yet the firms ignored those inadequacies and failed to adopt appropriate measures to remedy those dangerous shortcomings.

144. Defendants BINANCE and POLONIEX also knew the funds were stolen while the funds remained at BINANCE and POLONIEX; and any reasonable compliance standards would have revealed that.

145. Moreover, Defendants BINANCE and POLONIEX each know or should have known that the assets stolen from Plaintiff and stored within their custody were indeed stolen; however, BINANCE and POLONIEX have undertaken no efforts to return those stolen assets to Plaintiff.

146. To fulfill its role in the conspiracy, Defendant BINANCE agreed to facilitate the laundering and ultimate dissipation of Plaintiff's stolen assets by:

(a) Accepting into, and maintaining in, the BINANCE accounts and wallets identified above Plaintiff's stolen assets despite being on notice that those funds were stolen;

(b) Declining to implement AML and KYC controls that would have required BINANCE to freeze the accounts and wallets identified above and report the suspicious activity to regulators and law enforcement;

(c) Allowing Defendant BULASA, Defendant LIAN, and Defendant LIN to launder and dissipate Plaintiff's stolen assets through BINANCE;

(d) Concealing material information from Plaintiff and her representatives;

(e) Refusing to freeze the BINANCE accounts and wallets identified above despite knowing the accounts contained Plaintiff's stolen assets; and

(f) Fraudulently maintaining that a plausible explanation exists for the patently-illegal laundering of Plaintiff's stolen funds through the BINANCE accounts and wallets identified above.

147. BINANCE knowingly assisted, furthered, encouraged and concealed the conspiracy by, among other things:

(a) Failing to implement or maintain a freeze on the BINANCE accounts and wallets after BINANCE was notified that those accounts/wallets were being used to move the proceeds of a crime;

(b) Refusing to provide Plaintiff's lawyers and investigators with, and thwarting their efforts to otherwise obtain, information necessary to prevent the further dissipation of Plaintiff's stolen assets;

(c) Knowingly permitting the continued use of its exchange to launder the proceeds of the crime, including by continuing to allow transfers of stolen cryptocurrency into the BINANCE accounts and wallets even after BINANCE was notified of the theft and that those accounts/wallets were being used to move the proceeds of crime;

(d) Failing to perform adequate customer due diligence and KYC procedures at the time Defendant BULASA and his agents opened accounts at BINANCE;

(e) Employing atypical policies related to the opening of accounts, deposits, and withdrawals, in that BINANCE allowed new users to open accounts and transact on the exchange without demanding from its accountholders any meaningful identification or KYC information;

(f) Enabling cryptocurrency thieves like Defendant BULASA to open an unlimited number of anonymous trading accounts on its exchange, thereby hindering detection and identification of the thieves;

(g) Failing to utilize adequate AML transaction monitoring software systems to review and flag the suspicious money laundering transactions on its exchange that were involved in the theft of Plaintiff's assets; and

(h) Failing to file the requisite SARs tied to the suspicious money laundering transactions on its exchange that were involved in the theft of Plaintiff's assets.

148. To fulfill its role in the conspiracy, Defendant POLONIEX agreed to facilitate the laundering and ultimate dissipation of Plaintiff's stolen assets by:

(a) Accepting into, and maintaining in, the POLONIEX accounts and wallets identified above Plaintiff's stolen assets despite being on notice that those funds were stolen;

(b) Declining to implement AML and KYC controls that would have required POLONIEX to freeze the accounts and wallets identified above and report the suspicious activity to regulators and law enforcement;

(c) Allowing Defendant BULASA, Defendant LIAN, and Defendant LIN to launder and dissipate Plaintiff's stolen assets through POLONIEX;

(d) Concealing material information from Plaintiff and her representatives;

(e) Refusing to freeze the POLONIEX accounts and wallets identified above despite knowing the accounts contained Plaintiff's stolen assets; and

(f) Fraudulently maintaining that a plausible explanation exists for the patently-illegal laundering of Plaintiff's stolen funds through the POLONIEX accounts and wallets identified above.

149. POLONIEX knowingly assisted, furthered, encouraged and concealed the conspiracy by, among other things:

(a) Failing to implement or maintain a freeze on the POLONIEX accounts and wallets after POLONIEX was notified that those accounts/wallets were being used to move the proceeds of a crime;

(b) Refusing to provide Plaintiff's lawyers and investigators with, and thwarting their efforts to otherwise obtain, information necessary to prevent the further dissipation of Plaintiff's stolen assets;

(c) Knowingly permitting the continued use of its exchange to launder the proceeds of the crime, including by continuing to allow transfers of stolen cryptocurrency into the POLONIEX accounts and wallets even after POLONIEX was notified of the theft and that those accounts/wallets were being used to move the proceeds of crime;

(d) Failing to perform adequate customer due diligence and KYC procedures at the time Defendant BULASA and his agents opened accounts at POLONIEX;

(e) Employing atypical policies related to the opening of accounts, deposits, and withdrawals, in that POLONIEX allowed new users to open accounts and transact on the exchange without demanding from its accountholders any meaningful identification or KYC information;

(f) Enabling cryptocurrency thieves like Defendant BULASA to open an unlimited number of anonymous trading accounts on its exchange, thereby hindering detection and identification of the thieves;

(g) Failing to utilize adequate AML transaction monitoring software systems to review and flag the suspicious money laundering transactions on its exchange that were involved in the theft of Plaintiff's assets; and

(h) Failing to file the requisite SARs tied to the suspicious money laundering transactions on its exchange that were involved in the theft of Plaintiff's assets.

150. Each of the defendants acted in concert in furtherance of his/its role in the common plan to steal, launder, and dissipate Plaintiff's cryptocurrency assets.

151. As a direct and proximate result of Defendants' participation in, and furtherance of, the conspiracy; Plaintiff has suffered damages.

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands entry of a judgment against Defendants JERRY BULASA, an individual; DONG LIAN, an individual; DANYUN LIN, an individual; BINANCE HOLDINGS, LTD. d/b/a Binance, a foreign company; POLONIEX, LLC, a Delaware limited liability company; and POLO DIGITAL ASSETS, LTD., a foreign company; for damages, including compensatory damages, interest, expenses, and any other relief the Court deems just and proper.

## COUNT V – IMPOSITION OF A CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS
**[AGAINST TD BANK]**

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-109 above, and further alleges:

152. Defendant BULASA, Defendant LIAN, and/or Defendant LIN are the beneficiaries of funds that were wrongfully misappropriated, converted, and stolen from Plaintiff.

153. Although Plaintiff transferred to the ***8000 and ***2161 Accounts at TD BANK a sum total of Two Hundred Ten Thousand Dollars ($210,000.00), the amount of cryptocurrency transferred in return by Defendants LIAN and LIN was less than the cash equivalent for which Plaintiff had paid.

154. Upon information and belief, TD BANK holds some or all of the funds wrongfully taken from Plaintiff.

155. Any and all monies being held by TD BANK must be held in trust for Plaintiff's benefit, as Defendants LIAN and LIN are not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

156. Any and all funds held by TD BANK must be disgorged to Plaintiff's benefit, as Defendants LIAN and LIN are not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands imposition of a constructive trust to be effectuated by Defendant TD BANK, N.A., a national banking association; and full disgorgement of all funds in TD BANK's possession, custody, or control that were wrongfully misappropriated, converted, and stolen from Plaintiff; and an award of interest, costs, and any other relief the Court deems proper.

## COUNT VI – IMPOSITION OF A CONSTRUCTIVE TRUST AND DISGORGEMENT OF FUNDS
**[AGAINST ABACUS BANK]**

Plaintiff re-alleges, and adopts by reference herein, Paragraphs 1-109 above, and further alleges:

157. Defendant BULASA and/or Defendant LIAN are the beneficiaries of funds that were wrongfully misappropriated, converted, and stolen from Plaintiff.

158. Although Plaintiff transferred to the ***0334 Account at ABACUS BANK a sum total of One Hundred Eighty-Six Thousand Dollars ($186,000.00), the amount of cryptocurrency transferred in return by Defendant LIAN was less than the cash equivalent for which Plaintiff had paid.

159. Upon information and belief, ABACUS BANK holds some or all of the funds wrongfully taken from Plaintiff.

160. Any and all monies being held by ABACUS BANK must be held in trust for Plaintiff's benefit, as Defendant LIAN is not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

161. Any and all funds held by TD BANK must be disgorged to Plaintiff's benefit, as Defendant LIAN is not entitled to the benefit of wrongfully misappropriated, converted, and stolen funds and cryptocurrency assets that were taken from Plaintiff.

WHEREFORE, Plaintiff DIVYA GADASALLI, an individual, demands imposition of a constructive trust to be effectuated by Defendant ABACUS FEDERAL SAVINGS BANK, a federal savings bank; and full disgorgement of all funds in ABACUS BANK's possession, custody, or control that were wrongfully misappropriated, converted, and stolen from Plaintiff; and an award of interest, costs, and any other relief the Court deems proper.

**DEMAND FOR JURY TRIAL**

Plaintiff hereby demands a trial by jury on all claims so triable.

**RESERVATION OF RIGHTS**

Plaintiff reserves her right to further amend this Amended Complaint, upon completion of her investigation and discovery, to assert any additional claims for relief against Defendants or other parties as may be warranted under the circumstances and as allowed by law.

Respectfully submitted,

**SILVER MILLER**
*Counsel for Plaintiff Divya Gadasalli*
4450 NW 126th Avenue - Suite 101
Coral Springs, Florida 33065
Telephone: (954) 516-6000

By: */s/ David C. Silver*
DAVID C. SILVER
Florida Bar No. 572764
E-mail: DSilver@SilverMillerLaw.com

**CERTIFICATE OF SERVICE**

**I HEREBY CERTIFY** that a copy of the foregoing was electronically filed with the Clerk of Court on this 20th day of May 2022 by using the CM/ECF system and that a true and correct copy will be served via electronic mail to: **ALLISON CARROLL, ESQ.**, DUANE MORRIS, LLP, *Counsel for Defendant TD Bank, N.A.*, 100 Crescent Ct. - Suite 200, Dallas, TX 75201, E-mail: ACarroll@DuaneMorris.com; **AMANDA L. COTTRELL, ESQ.**, SHEPPARD MULLIN, *Counsel for Defendant Abacus Federal Savings Bank*, 2200 Ross Avenue - 20th Floor, Dallas, TX 75201, E-mail: ACottrell@SheppardMullin.com; **RYAN SQUIRES, ESQ.**, SCOTT DOUGLASS MCCONNICO LLP, *Counsel for Binance Holdings, Ltd.*, 303 Colorado Street - Suite 2400, Austin, TX 78701, E-mail: rsquires@scottdoug.com; and **KAREN R. KING, ESQ.**, MORVILLO ABRAMOWITZ GRAND IASON & ANELLO, P.C., *Counsel for Binance Holdings, Ltd.*, 565 Fifth Avenue, New York, NY 10017, E-mail: kking@maglaw.com.

*/s/ David C. Silver*
DAVID C. SILVER



**SILVER MILLER**
4450 NW 126th Avenue - Suite 101 • Coral Springs, Florida 33065 • Telephone (954) 516-6000
www.SilverMillerLaw.com